

Domain: 192.168.0.109

Vulnerability Name	Insufficient Anti-automation(Login brute force attack)
Severity	8.1 - High
CVSS Score	Base Score: 8.1 High CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Description	The "insufficient anti-automation" weakness in a login page refers to a lack of effective measures to prevent automated or scripted attacks. This weakness makes it easier for attackers to carry out brute force attacks. This method relies on the sheer computing power and automation to repeatedly attempt different combinations until a successful login is achieved. Observations: While testing the we have observed that there is no CAPTCHA enabled on the login form. By performing the multiple unsuccessful login with a known username and a random password we have observed that there is no account lockout policy was enabled for user account.
Attack Scenario	Attack Scenario: As an attacker we have performed a brute force attack on the login page with a specially crafted password dictionary and we are able to successfully login into the known user account by guessing the correct password. Impact: by performing the "brute force attack" on a login page, an attacker systematically tries all possible combinations of usernames and passwords until they find the correct ones.
Vulnerable Location	http://192.168.0.109/dvwa/vulnerabilities/brute/
Vulnerable Parameters	Login Form
Reproduction Steps	1.Access the application login page 2.Login page URL: http://192.168.0.109/dvwa/vulnerabilities/brute/ 3.Enter known user name and a random password, click on the login button. 4.Observe that there is no CAPTCHA enabled on the login form. 5.Try to log into the application by inserting the random passwords to guess the correct password. 6.After a certain number of unsuccessful login attempts enter user name and correct password. 7.Observe that the application is successfully logged in without locking out the user account. 8.Which means that there is not account lockout policy was enabled.
Remediation	1. Enable OTP - 2FA or MFA 2. Enforce Strong password policy - then users will set Strong passwords to their accounts. 3. Enforce Account lockout policy - after a certain number of unsuccessful login attempts 4. Enforce Password expiration policy - Changing passwords regularly. 5. Do not allow the users to reuse their own old/current password. 6. Enable CAPTCHA and reCAPTCHA - strict implementation and validation of CAPTCHA 7. Do not allow users to set a password of weak pattern - ex: Username@123
Sample Code	N/A
Reference	Link1 Link2

Proof of concept:

⚡

3. Intruder attack of 192.168.0.109 - Temporary attack - Not saved to project file

—□×

AttackSaveColumns

ResultsTargetPositionsPayloadsResource PoolOptions

Filter: Showing all items?

Request ^	Payload	Status	Error	Timeout	Length	Comment	
99	EcMcBa	200	☐	☐	4885		
100	PEfjyf1iO2	200	☐	☐	4885		
101	password	200	☐	☐	4951		

RequestResponse

PrettyRawRender\nActions ▾

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area admin

Paused